SECTION 4. NETWORK START-UP AND OPERATION GUIDELINES

INTRODUCTION

When operating a LAN, certain steps should be taken so that it will run efficiently and with minimum interruption to LAN users. This section provides guidelines to insure smooth operation of the LAN designed in section 3. This section is divided into three parts. The first part provides guidelines for selecting the LAN staff and determining the appropriate composition of that staff. The first part also describes guidelines for both staff and LAN user training. The second part provides guidelines on preparing and installing the hardware and software on a LAN. The last part of this section provides guidelines on the management of a LAN.

PART 1. STAFFING AND TRAINING GUIDELINES

STAFFING

One of the first steps in LAN operation is the establishment of a LAN staff. The number of people and the positions required to support the LAN will vary directly in relation to network size. For a large network, there should be a ratio of two to three LAN staff members for every 100 LAN users. This ratio may increase as LAN size decreases, due to the economy of scale. In any case, it is strongly recommended that a minimum of one senior administrator, one junior administrator, one technician, and one LAN user assistance operator be assigned full-time to support the LAN and LAN user services. As shown in figure 4-1, one senior administrator will supervise a number of junior administrators, technicians, and LAN user assistance operators. Generally, one full-time junior administrator can effectively manage up to 10 LANs (with the appropriate test, measurement, and diagnostic equipment (TMDE)), and one full-time technician can handle up to 100 LAN users and workstations.

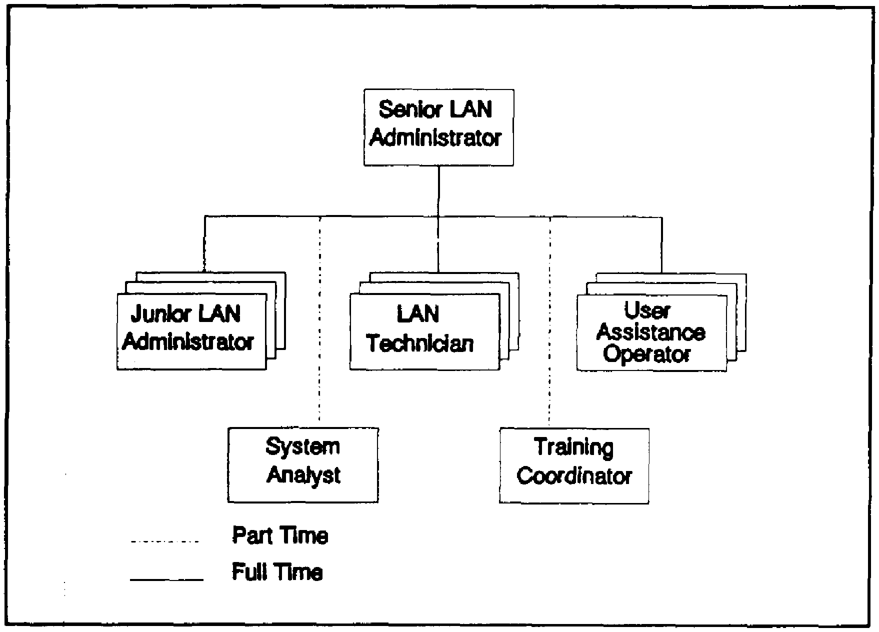

FIGURE 4-1. Sample LAN staff organization.

In addition to these full-time positions, a systems analyst/design engineer and a training coordinator should be assigned for part-time LAN support, depending upon requirements. Personnel for these positions may be drawn from the current staff or from contractor support.

Careful selection of staff should be made using the following guidelines.

Senior LAN administrator

Senior LAN administration duties include supervision of LAN installation and the day-to-day operation of all LAN support functions. This includes supervision of the LAN user assistance branch, which is responsible for managing, monitoring, and resolving information management problems. It is essential that the senior LAN administrator be identified early, to ensure participation in decisions concerning design and configuration of the LAN, management software, and test tools needed to accomplish the task. The senior LAN administrator sets LAN use and operations policies, establishes repair and upgrade procedures, and is the central responsible authority for LAN users in identifying and eliminating LAN viruses.

A critical responsibility of the LAN administrator is to see that file backups occur. All files that are maintained on LAN servers should be backed up on a regular schedule. A minimum schedule should be to backup daily and weekly. In this case, individual files would be needed for each day of the week. On Monday, Tuesday, Wednesday, and Thursday, the procedure should be to backup only modified files (Incremental backup). On each Friday, a full system backup should be performed. The full system backup files should be archived to provide the capability to restore data that might be lost by a catastrophic failure. Archived files should be identified with the system name, date, period covered, and the name of the person who actually performed the backup. All daily and weekly backup files should be stored at a separate location for disaster recovery purposes. The length of time that archived files would be retained should be at the discretion of the Director of Information Management (DOIM).

This position requires a thorough knowledge of the appropriate Institute of Electrical and Electronics Engineers (IEEE) standards and a supplemental knowledge of Government Open Systems Interconnection Profile (GOSIP), as these standards apply to LANs. Experience in managing LAN installations and a working knowledge in LAN design, cable plant installation, and LAN integration and management is desired.

The senior LAN administrator should have at least 4 years LAN experience and a degree in computer science, electrical engineering, management information systems, or a related field.

Junior LAN administrator

The junior LAN administrator adds and deletes LAN users on the network; assigns network addresses and file access privileges; installs various LAN components and support application packages; uses management tools to monitor, detect, and report problems; initiates corrective action when necessary; performs scheduled backups; and maintains the resource inventory as equipment is received for the LAN. This position requires the ability to use the available tools to develop trend and historical usage data.

The junior LAN administrator should have at least 2 years LAN experience and a minimum of 2 years formal training in information systems or a related field.

LAN (electronics) technician

The LAN technician is responsible for installing, maintaining, and repairing electrical devices or circuits. The technician will be responsible for installing and maintaining the LAN components including network cards, hubs, bridges, routers, gateways, workstations, cables, connectors, and microcomputers. The LAN technician maintains as-built drawings of floor plans and make changes to include cable and equipment locations.

The LAN technician should have at least 4 years experience in installation of telecommunications and LAN equipment and a minimum of 2 years formal training. Current knowledge of microcomputer devices, peripheral components, test equipment, and LAN procedures is essential.

LAN user assistance operator

The LAN user assistance operator is the focal point for LAN user interaction in terms of network and telecommunications problems. The LAN user assistance branch is open during normal duty hours with the capability to forward calls after duty hours to a centralized location where a determination is made as to the criticality and sensitivity of the problem.

The assistance branch should be staffed with knowledgeable system experts who can assist LAN users in resolving information management problems in the networking, application, and telecommunication arena. The LAN user assistance operator is responsible for logging in and monitoring problems and for generating trouble tickets for the appropriate information management support staff to resolve. Additionally, the LAN user assistance operator is responsible for interfacing and coordinating with the designated contractor (maintenance) for the repair of hardware equipment as required.

The LAN user assistance operator should have at least 2 years experience in LAN installation and applications. A knowledge of the course material presented in a LAN training classes is essential.

Systems analyst/ design engineer

The computer systems analyst/design engineer is responsible for:

1. Analyzing the requirements and selecting the network approach to provide the necessary service(s).

2. Ensuring that system setup and programming meet the configuration requirements of the design.

3. Verifying that the installation of equipment is complete and the equipment is fully functional prior to operational activation and assignment to the system administrator.

4. Modifying any existing networks for additions, changes, and updates.

The systems analyst/design engineer should have a degree in computer science or a related field, 5 years experience in systems design and analysis of LANs, and a thorough knowledge of the appropriate IEEE standards and GOSIP.

Training coordinator

The training coordinator is responsible for developing and conducting ongoing training courses related to the LAN.

The training coordinator should have 3 years training experience and instructional expertise in network operating systems, electronic message systems, communications systems, and microcomputer application software such as word processing, spreadsheets, database, and menus.

TRAINING

Ongoing training should be provided for the LAN staff and the LAN users.

Administrative design engineer

Training should include both theory and practical hands-on instruction tailored to the installed network. Courses should include duties of the LAN administrator; operating system features and parameter settings; LAN components and features; LAN procedures including access, file management, libraries, security methods, and space management; and familiarization with LAN management.

Technician training

Training should include instruction on installing, operating, and maintaining LAN components.

LAN user training

Successful LAN user training lessens the burden on the LAN administrator/user assistance operator during the day-to-day operations. End user training should provide instruction on how to interact with the network operating system, use of the application software, and hardware provided. Since the system should provide a seamless and transparent interface to the network for the LAN user, this training should take only a few hours. It is important that the LAN users are introduced to the features of the network, are run through the menus, and are shown general LAN concepts. Ideally, this training should be presented in a hands-on format. Issues to be covered should include:

1. Login and logoff procedures
2. Directory and access file rights
3. Using menus
4. Operation of personal computers (PC) and printers
5. How to access print queues
6. How to use applications

7. Virus protection

8. How to use the help desk

9. File backup.

PART 2. LAN INSTALLATION GUIDELINES

SITE PREPARATION

Preliminary engineering and site concurrence documentation should be prepared during the initial survey. Preliminary engineering consists of obtaining or developing drawings and collecting information pertinent to the communications closet. The Site Concurrence Memorandum should record the agreements concerning site preparation and other installation support reached with the LAN user during the site survey and through formal and informal correspondence subsequent to the site survey.

CABLE INSTALLATION

For cable installations, the same general philosophy exists for all buildings - **follow the routes established by the telephone installations.**

Whenever installing cable it is important to make sure:

1. There is space for both the present installations and future expansion.

2. Cable installation will meet applicable fire and safety regulations.

3. Once installed, the cable will be readily accessible for easy maintenance.

Installation rules and regulations

Installation of cable can be performed by in-house technical staff or contractor personnel and should be in accordance with FM 11-487-3. For additional information on cable installation techniques, consult the Army Field Manuals 11-486-5 and 11-487-5, -9, -13, -14, -15, -17, -18, and -19, or Air Force Inside Plant Cable Installation Instructions TO 31-10-2, -6, -7,-11, -12, -13, and -16.

The following is a quick checklist for LAN installations.

1. Choose cable routes: floor, ceiling, or walls; and choose cable routing method: zone, conduit, or point-to-point.

2. Complete communications closet preparation. Install or upgrade conduits, cable trays, or raceways from communications closet to cable routes.

3. Install all cables. Terminate each wire and fiber at both ends of every cable in appropriate patch panels or user information drop wall plates.

4. Tag and label all cables in accordance with FM 11-486-5. Each cable should be uniquely identified. Create or update plant-in-place drawings of all cables installed. Create or update a Cable Connection Database to record user signal paths and maintain a record of all moves, adds, and deletes. This database should include all patch panel connections and cable identification tags.

User cable distribution

There are three basic methodologies for installing user cable between the communications closet and users located on the same floor: in the ceiling, along the wall, or under the floor. when selecting the cable route, the designer should weigh safety, flexibility or rearrangement, initial cost, cost of later additions or alterations, access to the communications closet, and general aesthetics. Cable routed under a raised floor or in a drop ceiling may need to be plenum rated, since these areas often contribute to office air flow. User cable should not be in the same cable tray or conduit as electric power wiring.

Ceiling installation

When installing cable in the ceiling, space requirements and safety codes should be considered. If ceilings are used as air return paths for heating and air conditioning, cables should either be enclosed in approved conduit or channel, or be plenum rated cable. Also, the more cables installed in the drop ceiling, the greater the combined weight; unused cable should be removed to reduce excess weight. Care should be taken to properly dress the cables. where many cables will be run together, cable should be installed in cable trays suspended from the roof/ceiling to minimize weight on the drop ceiling.

There are three basic ceiling distribution methodologies:

1. Zone

2. Raceway

3. Poke-through.

Zone

With zone distribution, the room space is divided into zones. The cables are then run in bundles from the wiring closet to the center of the zone. From the center of the zone, cable is fanned out to walls or utility columns.

Raceway

With raceway distribution, large raceways or cable trays (installed like a series of interconnected suspension bridges hung from the roof) bring the cables to the center of the area. Feeder raceways distribute cables to user locations.

Note: Raceways shall be installed in accordance with applicable electric codes.

Poke-through

With poke-through distribution, cable is run in the ceiling of the level beneath the user and then is "poked through" to the user location. This is an inexpensive method but can weaken the floor structure and violate fire and safety codes.

Wall installation in conduit

Wall installation should be done in conduit. This is because installing cables along the walls of passageways exposes the cables to wear and tear of people passing by, and exposes people to any risk from the cables. With conduit distribution, each group of cables is run in a continuous conduit from the wiring closet to the desired outlet. With this method, distribution is difficult and expensive to rearrange but provides a direct connection and complete protection for cables. Wall conduit installation should only be used when the outlet locations are permanent, device densities are low, and flexibility is not required. This technique is also used for cable run along walls. In older buildings that have neither raised floors nor drop ceilings, conduit or enclosed cable trays run along the walls is the most common method of cable installation.

Floor installation

There are two basic floor installation methodologies:

1. Underfloor duct

2. Raised or access floor.

Underfloor ducts

The underfloor ducts are usually installed while a building is undergoing construction. These ducts are covered metal channels very much like heating ducts. This methodology incorporates straight ducts, curved elbow ducts, and junction boxes where ducts intersect at right angles. The junction boxes act as pulling and repairing points and are usually accessible through tiled or carpeted floor. This approach provides convenient cable routing, but is expensive and typically only used when the building is first constructed.

Raised floor

With a raised floor, the floor stands on pedestals, and any section can be removed for access to the cable beneath. Raised floors are easy to install and repair and provide ease in rerouting underfloor cable; however, they are expensive. With the flexibility of raised floor cable routing, cables can either be bundled and routed in zones, or individual cables can be run point-to-point. The bundled, zone cable routing, similar to ceiling zone routing, takes more initial work and cable, but is more organized and easier to maintain than point-to-point. Point-to-point routing is easy to install, but confusing to maintain, with a tendency towards tangling.

Backbone cable distribution

When running backbone cable between the building distribution frame (BDF) closet and communications closets on the same floor, the cable should be routed along the same paths as user cable or telephone cable. Try to route the backbone cable so that it will not be disturbed when additions or repairs are made in the user cabling or telephone cabling. Any fiber optic cable should be routed and installed carefully to prevent stretching or breaking of the fibers. Unlike user cable, which contains both fiber optic strands and twisted-pair copper wire, backbone cable can be routed near electrical power or noise sources, since it contains no copper wire.

For new buildings or major renovations, consider adding a second cable with 12 single-mode fibers beside each backbone cable. These single-mode fibers will be left dark until required by new technologies.

To install the backbone cable between floors, there must be an opening in the floor between the wiring closets on each level. Since plenum rated backbone cable is recommended in this document, the backbone cable can be routed through air ducts, vertical shafts, or crawl spaces. Three common methods are usually employed.

1. Slots or sleeves

2. Conduits

3. Trays.

Slots or sleeves are rectangular openings that enable cable to pass through. These slots should be fire stopped (plugged with fire retardant materials) to prevent them from being a possible fire path. Conduit is either electrical metallic tubing, rigid metal, or rigid polyvinyl chloride (PVC) pipe. Trays are placed in the ceiling to provide a pathway for the cable. The cable should be plenum rated when run in areas that can induce a fire hazard.

When wiring closets are vertically aligned, a means should be provided to pull cable above and in line with the sleeves or slots. When closets are not vertically aligned, a more circuitous route will have to be designed. To meet safety standards, pathways should not be located in elevator shafts, unless appropriate steps are taken to protect the cable.

User Cable Connection Database

A cable connection database should be used to record the cable/cross connect path from each LAN user into the port on the hub that services them and the backbone cabling between communications closets. The database can be organized into three sections: hub port to patch panel pinout connections, patch panel cross connects, and cable run from the communications closet to the user information drops. An optional fourth section, listing related user names to hub port connections, would aid in correlating network sniffer and hub Simple Network Management Protocol (SNMP) data with the LAN user data traffic. Each entry should detail the location of each end of the cable, the unique identifier on the cable tag, and the cable type and length.

The hub to patch panel section would include the name or location of the communications closet, the number of the hub if more than one is present, the number or unique identifier of the input/output *(I/O)* module, the port number on the module, the patch panel to which the patch cord is connected, and the numbers of the connectors or pins to which it is connected.

The patch panel cross connect section should list the name or location of the communications closet, the patch panels involved, the equipment side connectors or pins, the user side connectors or pins, and the unique identifier of the user cable connected to the patch panel.

The user cable section should list the originating communications closet, patch panel, connectors or pins on the patch panel, floor and room number of the information drop, location within the room of the information drop, and name of user currently connected to the information drop.

The optional fourth section, relating user names to hub port connections, would include a list of current LAN users and what hub, I/O module, and port they are currently connected to.

Cable installation testing

All cables should be tested before being used in the LAN. Cable problems found before LAN start-up will save considerable troubleshooting effort after LAN start-up. Minimal testing of unshielded twisted-pair (UTP) cable should include tests for continuity and shorts. Minimal testing of fiber optic cable should measure the optical power loss. Additional testing of UTP cable should include frequency response, pair-to-pair noise immunity, and a time domain reflectometer to detect and locate defects or irregularities. The optical fiber should be tested for modal dispersion and cable flaws.

EQUIPMENT INSTALLATION

The LAN equipment can be installed in the communications closets once the user and backbone cable has been installed and the closets have been prepared according to the Site Concurrence Memorandum (with any additional racks/cabinets installed, dedicated 20 amp power circuit and receptacle(s), adequate chassis grounds, and ventilation). To prevent electrostatic discharge (ESD) damage to any electrical equipment, grounded wrist straps or other approved ESD protection procedures should be used. For a layout of an ideal communications closet in terms of equipment spacing, including an optional uninterruptible power supply (UPS) and an external fiber distributed data interface (FDDI) bridge, see figure 4-2.

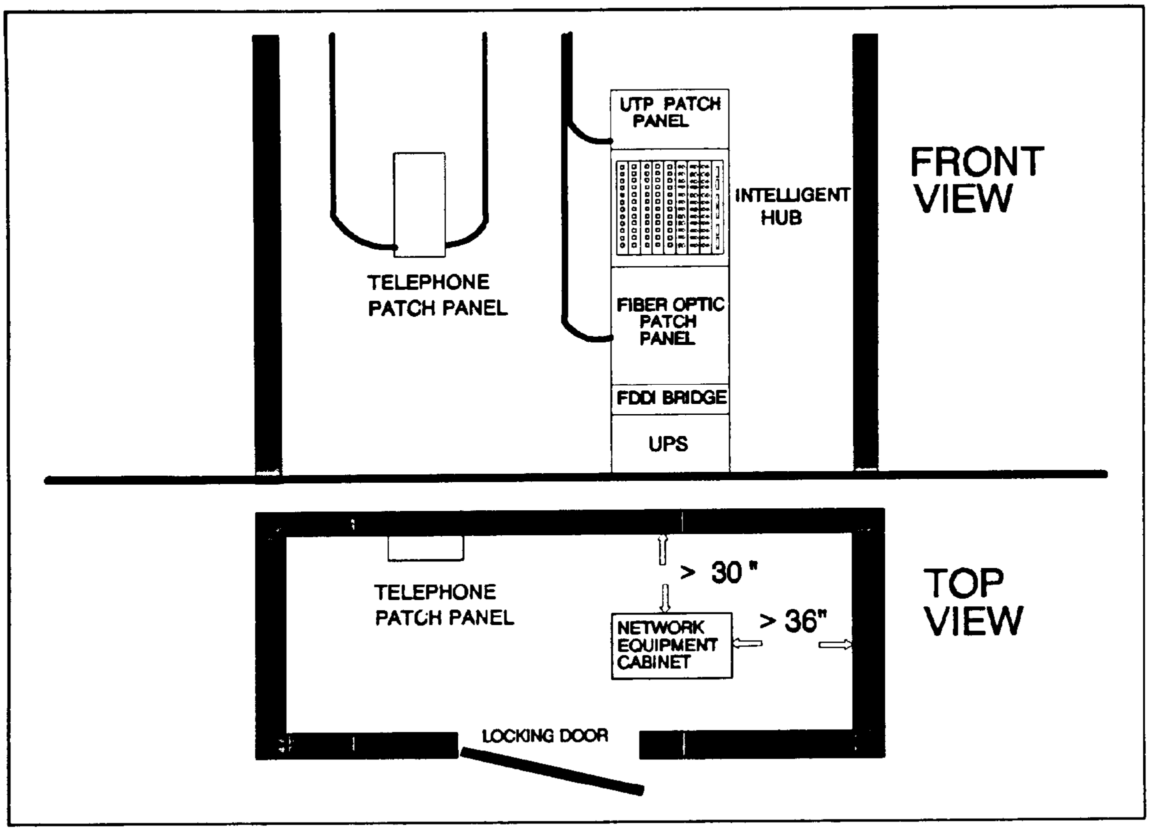

FIGURE 4-2. Ideal communications closet layout.

Communications closet equipment

Equipment installation within the communications closet should first include the assembly of intelligent hubs, patch panels, and any additional equipment such as external bridges, transceivers, and UPSs into LAN racks/cabinets. Placing the fiber optic patch panel above the hub and placing the UTP patch panel below the hub should minimize breakage of fiber patch cables. All user and backbone cables should be routed, bundled, and tie wrapped to prevent flexing and breakage. All power cords should be connected to power strips or should be directly connected to the dedicated LAN power receptacles. If a UPS is used, the LAN equipment should be connected to the power outlet of the UPS, and the UPS should be connected to the LAN power outlet.

The next step should be the installation of assembled hubs and any non-rack mounted equipment. If the hub module placement is not critical for hub backplane interconnection or network segmentation, then similar hub modules should be grouped together in order to simplify cable routing and maintenance.

After hub installation, the backbone fiber optic cable should be connected to the bridging module. If an external fiber to attachment unit interface (AUI) transceiver is required, the transceiver AUI cable should be connected to the bridge AUI port, and the backbone fiber patch cables should be connected to the transceiver fiber ports. If an external FDDI bridge is used, the backbone fibers should be connected to the bridge FDDI ports, and the bridge Ethernet port should be connected to the hub Ethernet backplane through a UTP or AUI port on an interface module. A special AUI cable may be needed. If FDDI user connection modules are used, the backbone FDDI fibers should be looped from the bridge FDDI ports to the hub FDDI module ports and back to the BDF. Figure 4-3 shows the backbone fiber optic connections for a hub with UTP, 10BaseF, and FDDI modules; an FDDI to Ethernet bridge with UTP Ethernet connection; and a BDF fiber optic patch panel.

The manufacturer's instructions should be followed when configuring the switch settings or software settings for the hub, modules, and bridges. The hub and bridge should be self-configuring. All setup settings should be recorded to simplify later maintenance.

Servers

When selecting a location for server installation, the degree of physical access control required by the application should be considered. Prior to the assembly and installation of any server, a parts inventory should be performed to verify that nothing is missing. Attributes such as brand and model of

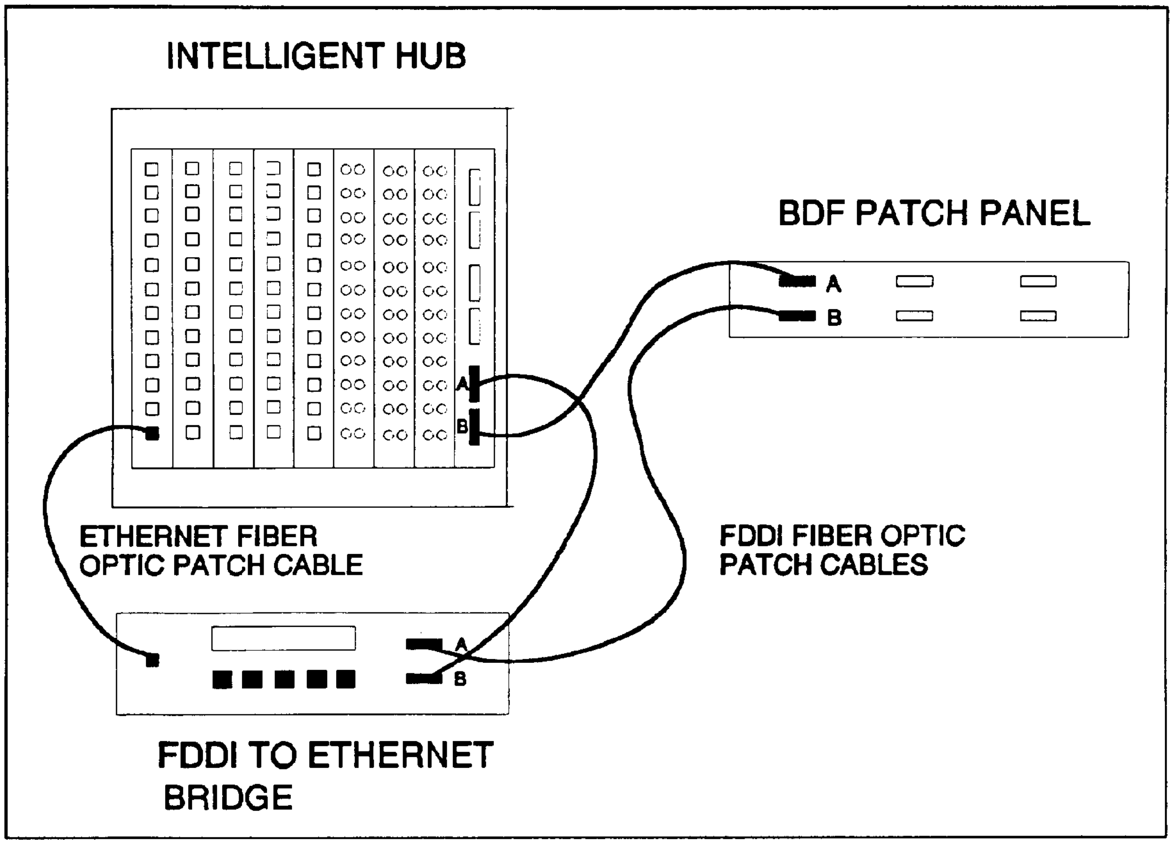

FIGURE 4-3. Possible FDDI backbone connection.

computer, type of hard disk and size, and type and amount of memory should be documented for each server and placed in a file with the inventory. If any warranty cards are included, they should be filled out at this time and returned to the vendor.

During the physical installation process, ESD protection procedures and manufacturer's instructions should be followed. Interrupt and I/O addresses of all cards should be documented. Then the network interface card (NIC) should be installed. If the backup system (tape, compact disk read only memory (CD ROM), and so forth), requires a card, that card should be installed. The power circuit used for the server should be used exclusively for the server. Once the UPS is connected to the receptacle, the UPS functionality should be evaluated according to the manufacturer's directions. After the server is connected to the UPS, the server and UPS should be checked to see that they operate as expected. Once the LAN cable is connected to the server, appropriate test methods should be used as provided by the network operating system (NOS) to validate the server connectivity on the LAN.

Workstations

A NIC is used to convert a standard PC to a network workstation. The NIC is installed into one of the PC bus expansion slots and provides the dedicated connection between the computer and the LAN server. while the mechanics of setting up the NIC are relatively easy, this is best accomplished by the LAN technician. A record of all the various settings for each terminal must be maintained to avoid conflicts in future installations and aid restoration of failed terminals.

SOFTWARE INSTALLATION

Network software must be installed in both the server and workstations that will reside on the LAN to provide proper network operation.

Server NOS installation

Before beginning installation of software, all software required should be on hand (for example, NOS software, LAN drivers, disk drivers, UPS monitoring software). The configuration list of hardware interrupts that was completed when installing the server should then be validated. A virus check should be run on all software before it is installed. Backup copies of the software to be installed should be made and the original disks stored in another location. The backup copies should then be used for installation. A unique name and network number should be selected for each server on the LAN. This may be identified by the LAN administrator as a part of configuration management. If the server is to be on the Internet, the internet protocol (IP) address should be identified. Follow the manufacturer's instructions to load the NOS software. Other communications protocol software should be loaded as desired, for example Transmission Control Protocol/Internetwork Protocol (TCP/IP). If network printers are to be used, software for accessing printers must be installed and configured.

In case the supervisor account is damaged or in-accessible, a secondary supervisor account should be created. A separate password and user identification should be created and assigned supervisor privileges. The LAN administrator, following NOS documentation, should create user accounts for all initial LAN users, including user names, user passwords, file access privileges, and default login scripts.

Workstation network software installation

Following the manufacturer's guidelines and NOS specific instructions, the network driver for the workstation should be created. A backup copy to be used on subsequent workstations should be made. Virus scan software should be installed and run on the workstation to ensure that it is virus free. After installing the driver on a user's workstation, the workstation should be brought up on the LAN and the connection validated. Other communication protocol software, such as TCP/IP, should be loaded.

ACCEPTANCE TESTING

A pre-cutover/post-cutover LAN acceptance test should be conducted in accordance with a government or contractor prepared test plan. Should the test plans be prepared by a contractor, they must be approved by the Government. As a general rule, the acceptance test consists of, but is not limited to, tests which verify the minimal points of functionality to be expected with a newly installed LAN. Each individual test should be a clear derivative of specifications made in the LAN design.

Test plans/procedures should be defined prior to the execution of any tests in a manner prescribed by the Government.

The quality and completeness of testing, the validation of the new LAN, and the accuracy/completeness of the acceptance test should remain with the Government.

Test equipment should be provided by the Government or the contractor. All equipment used should be in calibration and should display the date of the last calibration and next scheduled calibration date. A determination of who shall provide the test engineer and test personnel should be made during the formulation of test plans.

Pre-cutover test

Pre-cutover testing is performed after the installation of LAN hardware/software and prior to cutover. Testing should demonstrate LAN operability, conformance with contract requirements, and LAN readiness for cutover.

Specifically, pre-cutover testing should include:

- Connectivity tests. Connectivity tests verify local and remote, user-to-user/network-to-network LAN connectivity. Such tests examine file transfer, response/acknowledgement time, throughput, etc. Tests shall be performed from NIC-to-NIC/NIC-to-hub (end-to-end) on the LAN. Unused connections and cables installed for future connectivity shall also be tested.

- Intelligent hub/backbone tests. Intelligent hub/backbone tests verify in-system operability of intelligent hubs and other equipment contained in each wiring closet.

- Server tests. Server tests verify server in-system operability. Tests exercise the server’s memory, monitor, connectivity, hard disk (storage), floppy disk, keyboard, backup system/s (i.e., tape drive, CD ROM), network card, parallel card (printer), and UPS. In addition, server tests check file transfer, validate loaded software, and monitor protocols.

- Data transmission quality tests. Data transmission quality tests examine end-to-end data quality and reliability using a line monitor to document bit error rate (BER) and a network sniffer to monitor packet retransmission requests, runts, oversized packets, and garbled packets. Data transmission quality tests check for circuit connectivity and degradation.

- Network stability tests. Network stability tests check network error control and recovery. Tests include disconnecting nodes and powering systems up and down in the middle of network sessions.

- Stress tests. Applicable stress tests (e.g., thermal, power, and load tests) verify LAN functionality outside of standard/normal ranges of operability. Tests shall be incorporated as a function of the LAN requirements outlined in the purchase contract.

- Application tests. Application tests exercise the portion of the LAN software most directly related to the end user. Operation of the LAN application software will also test all elements of the network in normal modes of operation.

- Network management tests. Network management tests exercise the capability of network management software applications and tools installed on the LAN.

Post-cutover test

Post-cutover testing should be performed following the cutover, under actual operating conditions, with live and/or simulated traffic on the LAN for a failure-free period of 30 days. Testing should demonstrate that the typical application load will be supported. Simultaneous testing of infrastructure hardware/software is preferred but not required.

Test reports

At the completion of acceptance testing, a final test report should be developed along with the supporting data collected during testing. Reports should include requirements, test equipment used, results obtained, and any deviation from the original government approved test plan. It is recommended that the test data be copied onto floppy disks. Diskettes should be marked with the source of data, time of collection, and the test scenario involved and should be safely stored to be used as a benchmark for future reference.

PART 3. NETWORK MANAGEMENT GUIDELINES

Effective network management ensures the functionality of the LAN. LAN management tools should be purchased to assist the LAN staff in troubleshooting problems and maintaining a high level of service to the LAN users. These tools should be used by administrative staff to establish a logical map of the LAN during and after installation, as well as to help integrate any existing LANs with the new one. Once the map is complete, these tools can also help determine LAN resource allocation. Integration of network and data center management encourages efficient operation of the network with minimal disruption of services to LAN users.

To comply with the Government Network Management Profile (GNMP) - Federal Information Processing Standard (FIPS) Publication 179 in the area of systems management functions, a LAN implementation must satisfy the requirements as outlined in part 18, clause 8.3.2 of the Open Systems Environment (OSE) Implementors Workshop (OIW) Stable Implementation Agreements (IA), June 1992. In accordance with the GNMP, network management tools must provide for:

1. General management

2. Alarm reporting and state management

3. General event report management

4. General log controls.

5 ELEMENTS OF NETWORK MANAGEMENT

Network management tools in a LAN implementation should incorporate the five elements of the "Network Management for Department of Defense (DoD) Communications," MIL-STD-2045-38000. The five elements are summarized below.

Configuration management

Configuration management is the task of managing and documenting the hardware and software configuration of the LAN. Configurations to be managed include the cabling, equipment, software, NOS user accounts, and file backups. Personnel moves typically affect all of these areas at once. Up-to-date LAN documentation is invaluable for problem resolution, disaster recovery, and capacity planning. However, if discipline is not maintained in promptly updating the LAN documentation after changes occur, the documentation becomes useless. Specific components that should be managed and documented are as follows.

Cable

LAN staff should document the entire cable path, including cable numbers and pair assignments, from each user wall outlet to the LAN or BDF hub, in the Cable Connections Database. This documentation should include the department, name, and phone number of each LAN user to aid in problem resolution. This should be updated after every LAN add, move, or delete, or the database will gradually become useless.

LAN staff should also maintain records in the Cable Connections Database of all interhub and inter-LAN physical linkages such as patch panels, backbone cable pair assignments, and backbone cable locations. The inter-LAN records should also be updated after each inter-LAN cable change.

Equipment

LAN staff should document the inventory of equipment, including component modules. Switch settings, configuration parameters, and disaster recovery procedures should be documented. LAN staff should update the documentation immediately after each equipment move, add, delete, and update.

Software

LAN staff should document the inventory of software packages and component modules, including software installation, configuration parameters, and disaster recovery procedures. The documentation should be updated immediately after each software move, add, delete, and update.

NOS user accounts

LAN staff should document NOS user accounts, rights, and server access. This documentation should include the department, name, and phone number of the LAN users, as well as their node address. LAN staff should update the documentation for each personnel change. Network management-level passwords and security software should be documented. This documentation should be kept separately in a locked or secured room.

File backups

LAN staff should document the file backup procedures described in the LAN staffing section and should keep them updated. As they perform the backups, LAN staff should also update logs showing what was backed up and how the backup media were stored.

Fault management

Fault management is the process of identifying problems, collecting problem reports, tracing problem symptoms, investigating source problem causes, determining effective corrective action, and making repairs or system upgrade suggestions. It is important to discover and correct the underlying causes of network problems.

It is also important to establish policies and set priorities for investigation and repair activities. Will the fault isolation staff operate 24 hours a day, or only during standard duty hours, and with what level of staffing? What level of spares should be kept on hand? The LAN administrator should also set the priorities for investigating problem reports and for effecting expensive repairs or upgrades.

Problem collection and identification

To begin the fault management process, it is first necessary from all possible sources. Three prime sources are the LAN user assistance staff, the network performance management process (described below), and the network technicians. Since the problem may be intermittent or occur only during special circumstances, it is important to get a detailed description of the problem, where on the network it was discovered, and under what circumstances it occurs. Trouble report forms are usually a compromise between the level of detail desired by the fault management people and the level of detail that the LAN users are willing or able to provide. A form that is too complicated might discourage LAN users from reporting all problems.

Symptom identification

Before beginning the fault isolation process, the reported problem symptoms must be investigated and refined. For intermittent problems, the LAN staff should try to re-create the circumstances as closely as possible. If using a network sniffer or protocol analyzer, staff should start as close to the reported source of the problem as possible. Begin reducing the number of conditions needed to produce the symptoms. Staff should try to find the conditions that produce the greatest concentration of defects, checking for line noise or degraded signals on both sides of bridges, routers, hubs and other re-timing or re-transmission devices, and tracing garbled signals back to the location with the poorest signal quality. Staff should look for multiple problems that might be related or due to the same source cause.

Fault isolation

Once the symptoms have been clearly identified and the conditions that produce the error have been found, it is usually easy to determine the fault causing the observed symptoms. When possible, staff should use test equipment to verify the source of the problem. Staff should avoid indiscriminate swapping of cards or modules, or wiggling of cables, connectors, or cards. This will sometimes cause an intermittent failure to disappear for awhile, but the failure often comes back.

Determine source cause

Most network problems can be traced back to a causative agent. The fault manager should find out why the defect occurred in the first place. Then, both the defect and the source cause can be corrected to make sure that this defect does not happen again.

For instance, a LAN user that reports difficulty operating an application is found to be disconnected by the application because the packet timer is timing out. Instead of increasing the packet timer limit, the fault manager should instead find out why the packets are arriving late. The packets may be lost due to an over-loaded bridge, a routing table that sends the packets the long way around, a server with too many applications running at once, or a workstation that is too slow. Some problem causes will be simple and direct, such as failed NICs or broken or defective cables or connectors. However, even these may have source causes that if not fixed will lead to repeat failures later. The NIC may have been damaged by static discharge from people walking on carpeting or by voltage spikes in the ac power. The cable or connectors may be damaged by people walking on them or brushing against them, or by the cable catching on something.

Performance management

The function of performance management is to evaluate long-term behavior of the LAN. Performance management includes collecting and analyzing system statistics, tuning and controlling performance of the LAN based upon such analyses, and generating reports (both realtime and offline).

Accounting management

Accounting management tracks the network resources used by each network user. Standards for traffic data records, billing, bill reconciliation, and service order accounting are being developed within the International Standards Organization (ISO) community. Automatic message detail recording (AMDR) will be required in all switching units, but the format and elements are still in draft stages.

Security management

GNMP has identified five security services as the primary requirements for network management. These services are authentication, access control, confidentiality, integrity, and non-repudiation. GNMP discusses only access control and authentication, but the other three areas are expected to be included in later versions of the standard.

Make note that not all LANs will require all these services. Since the standards are not fully developed, security services are not readily available today. These security services may be provided at one or more of Open Systems Interconnection (OSI) layers 3, 4, and 7.

The network staff should look for the following security services when selecting a network management system (NMS).

Authentication

Authentication services verify the identity of the LAN user and the source of data. LAN subsystems that process BLACK (unclassified) data should have login and password authentication. For example, each LAN user should have a unique login name and password associated with it. The NMS should allow a LAN user three attempts at login. After the third unsuccessful attempt to login, the account would be disabled and the LAN user would be requested to contact the LAN administrator to validate user access.

NOTE: LAN subsystems that process CLASSIFIED or secure data should have security level, login, and password authentication, as well as audit trail and encryption services. The entire LAN has to be system high for the appropriate security level of classified data.

Access control

Access control services allow only access to those areas and resources for which the LAN user has authority. Both discretionary access control (DAC) and mandatory access control (MAC) policies should be used in accordance with DoD 5200.28-STD. These access rules define what data can be received from the LAN and what data can be transmitted over the LAN. Every attempt at data transmission should be verified against the rules before any action takes place. Access control should also be provided for read/write access to files and directories on the servers and hosts. The LAN administrator should be able to control access to network devices such as printers, plotters, and hosts. The NMS should provide access control to login, files, resources, programs, time of day, user, event, terminal identification, routing configuration, inactivity timeout, and time limits.

Data confidentiality

Data confidentiality services protect against unauthorized disclosure. Only those files assigned to a LAN user can be accessed by that LAN user. The implementation of this service is still being developed. It is anticipated that the standard will include ways to ensure that LAN users can be assured of the confidentiality of their files.

Data integrity

Data integrity services protect against unauthorized modification, insertion, or deletion of files (connectionless integrity). The implementation of this service is still being developed. It is anticipated that the standard will include ways that LAN users can be assured files that are sent to other LAN users will be received intact and without alteration of content. The incorporation of virus checking software should assist in the facilitation of this service. All computers and workstations on the LAN should be running virus scanning software.

Non-repudiation

Non-repudiation, with proof of origin, provides the recipient with proof of origin of data and protects against any attempt by the originator to falsely deny sending the data. Non-repudiation, with proof of delivery, provides the sender with proof that a message was sent and/or received. The implementation of this service is still being developed.